The metaverse: Navigating the evolving risk landscape for retailers

Whitepaper
July 2023

Produced in collaboration with:

BAYES BUSINESS SCHOOL
CITY, UNIVERSITY OF LONDON

LOCKTON®

Introduction

The world is changing at an unprecedented pace. With every generation comes new needs and expectations, as well as innovative concepts that often trigger rapid shifts economies and sectors. To sustain their competitiveness in this everchanging market, as well as ensure relevance to the evolving consumer base, businesses are in a constant race to be ahead of the commercial curve.

With technology acting as enabler for accelerated innovation, disruptors of tradition are constantly seeking methods for prompting change, whilst focusing on personalisation, creativity, and efficiency. The retail sector is a prime example for such change. From physical trading stalls, shopping centres, to e-commerce and online shopping, the sector is constantly evolving to increase efficiency and outreach, whilst elevating customer experience.

So, what is the "next big thing" within the retail sector? Considering the lack of sensory immersion involved in the browse and click online model, retailers are now pursuing new operational realms to overcome the static nature of online shopping. New realms? The metaverse. In 2022, a study done by TLT, a UK law firm, revealed that out of 100 top UK retailers, 12% are already using the metaverse, and 39% plan on using it in the future[1].

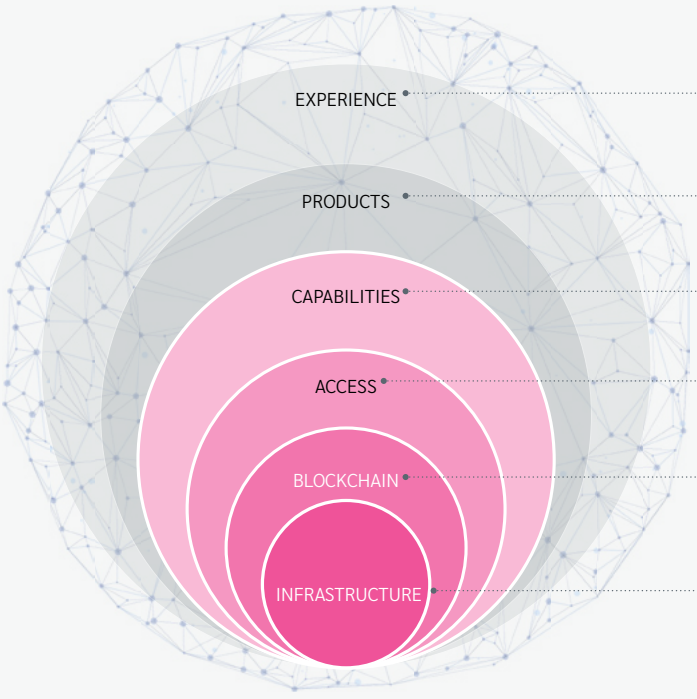
As the metaverse evolves, more retailers are expected to utilise the features and advantages offered. Hence, understanding the implications of this operational shift is crucial for mitigating any potential evolving or emerging exposures. **This white paper delves into describing the building blocks of the metaverse, whilst examining the associated risk management and insurance implications for retail businesses.**

In 2022, a study done by TLT, a UK law firm, revealed that out of 100 top UK retailers, 12% are already using the metaverse, and 39% plan on using it in the future.

Firstly, what is the metaverse?

The concept of a virtual, immersive, world is not new. It is rather a historic achievement that evolved alongside the most remarkable technology milestones over time. From the development of the first multisensory simulation and virtual reality (VR) headset in the 1960's, to the evolution of the internet from Web 1.0 to Web 3.0 between the 90's and now, the technological shift in the past decade in particular has been outstanding[2]. The intricacy and sophistication of the software and hardware developed, as well as the achievement of what we deemed as improbable "futuristic dreams" cannot be denied. The metaverse is essentially a by-product of decades' worth of innovation and non-traditional disruption.

It is the next ideation of the internet, a virtual dimension that mirrors our day-to-day realities. The metaverse is a "massively scaled and interoperable network of real-time rendered 3D virtual worlds, which can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications, and payments[3]". In simpler terms, an immersive digital space, which allows users to do things beyond the limits of reality from the comforts of their homes, in the physical world.



Metaverse Layers

Hybrid shopping Mixed reality Virtual events	Social gathering Gamification	Immersive content Digital interaction
Digital assets "Phygital" twin products	Digital spaces NFTs Visual search	Digital services Lenses Skins and avatars
Commerce Search	Marketplaces Currencies	Smart contract Co-creation
AR/VR hardware and software	Computing devices Apps	Websites
Cryptography Security	Identitiy	Ownership
Networks Server farms	Cybersecurity	Bandwidth

Source: https://www.ey.com/en_gl/consumer-products-retail/meet-customers-in-the-metaverse-to-unlock-lasting-value

As depicted in EY's representation of the metaverse above, there are multiple layers comprising the ecosystem needed for it to function[4]. At the heart of the metaverse lies the infrastructure and technologies, as well as blockchain, which enable the core capabilities and features differentiating these platforms. The access depends on the platform used, with some requiring augmented and virtual reality (AR/VR) hardware and software in addition to the usual computing devices and Apps/websites. The user's presence is digitally represented by an avatar, who's appearance and behaviour are controlled by the user.

The functions of the metaverse evolved significantly, with many starting off as gaming platforms to now becoming interactive societies where avatars can network, work, attend virtual events and concerts featuring global artists, shop, as well as carryout other day-to-day activities.

What opportunities does the metaverse offer retail businesses?

Although our understanding of the metaverse and Web 3.0 is still primitive, this space is expected to grow massively, potentially becoming an $8 trillion opportunity from a revenue and monetisation perspectives[5]. Operating in the metaverse could have various opportunities for a retailer. This includes increased customer outreach and interaction, access to a larger talent pool, less supply chain concerns, potential reduction in operational costs, as well as more tailored and targeted marketing strategies. With reference to TLT's study, retailers are using the metaverse for better customer engagement (12%), marketing (12%), creating experiences (9%), as well as for utilising the existing clubs and communities (8%). Fewer than 7% are using the platforms to sell physical products, and around 3% to sell digital products[6].

Retail businesses can utilise the immersive features to "drive gamified, social or event-driven shopping"[7]. Interest is created through indulging the customers in engaging experiences, which are not particularly available or as easily accessible in the real world. It also offers the opportunity to collaborate with customers to develop products that are tailored specifically to their preferences and needs.

Customers are increasingly using the metaverse to showcase their capabilities and talents, with more designing and creating their own digital products. Utilising the existing talent and encouraging collaborations will not only increase the brand's outreach, but also trigger innovation and growth as new perspectives and ways of thinking are introduced. This could also enhance brand reputation as customers are given space to influence the design and creation of the products they require and are seeking. This allows brands to develop a personal relationship with their customer base, which is driven by transparent communication and bilateral feedback.

With reference to TLT's study, retailers are using the metaverse **for better customer engagement (12%), marketing (12%), creating experiences (9%),** as well as for **utilising the existing clubs and communities (8%).**

Fewer than 7% are using the platforms to sell physical products, and around 3% to sell digital products.

How does the metaverse impact a retail business's risk landscape?

As retailers enter the metaverse, understanding the implications on their traditional risk landscape is crucial to appropriately identify and manage any emerging risks. Adequate risk management is necessary for ensuring the smooth and continuous operation of businesses, as well as safeguarding the organisation against unexpected and/or catastrophic losses. When asked, retailers identified cyber security and data protection (54% and 43% respectively) as the two main legal concerns within the metaverse. While 62% considered harassment and abuse as a growing concern, alongside IP infringement (54%), cross-jurisdictional issues (49%), as well as transparency and mis-selling (45%)[8].

The key risk areas are further detailed below. This list is by no means exhaustive or reflective of the overall risk landscape, as our understanding of the metaverse is still under development.

Digital assets

When thinking about the structure and features of a retail business on the high street, we consider the physical property, the location, the store front, the fittings and fixtures, the merchandise being sold, the hardware and technologies utilised, the staff etc. However, as a retailer shifts into the metaverse, and the physical assets are translated into digital assets, businesses should consider the emerging exposures.

In the metaverse, the transacted digital assets are non-fungible tokens (NFTs), which are "cryptographic assets on a blockchain with unique identification codes and metadata that distinguish them from each other"[9]. The ownership of the NFT is represented by a private key, which allows the owner to transfer and sell the represented asset. Any damage or loss to the server storing the private key will result in the loss of the associated NFT, with no means for retrieval. Hence, a retailer could lose control over their digital products if any damage occurs to the server.

Intellectual Property (IP)

The metaverse poses a myriad of IP issues, whereby the involved activities may involve infringement of IP rights due to NFTs being minted without the authorisation of the original content creator.[10] Retailers face the risk of online replicas and fakes being transacted across different metaverse platforms, which jeopardises the authenticity of the original digital products.

Brand protection is a significant concern, as brand value and reputation are vital to holding a competitive advantage within the retail sector. Consumer loyalty and building a 'brand fan base' for specific product lines has been evident among brands over the past decade, enabling businesses to lead customers to favouring one brand over another in an era of potential limitless options.

Moreover, with increasing collaborations between retailers and customers to co-create digital products, issues around ownership and rights may arise between the involved parties – who has the right to sell the developed products and has ownership over the original design/content?

Retail businesses must clarify any ambiguities over ownership and comprehensively detail all rights for both parties, to avoid any misuse or re-selling of jointly developed products.

Employees' safety and well-being

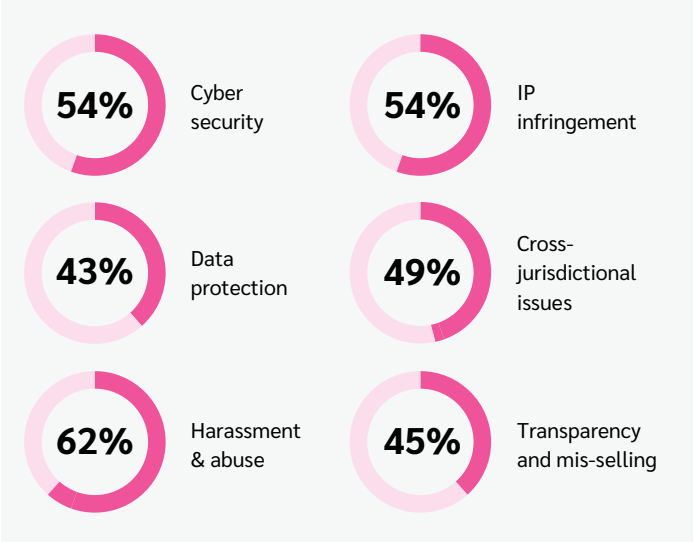
As retailers set up boutiques in the metaverse and expand their offering and outreach, more employees are expected to have a digital presence to ensure service delivery in the new operational environment. Despite their location, and the medium in which they operate, employers' must ensure consistent employee health and safety during their course of employment and work. That said, one of the main concerns is the inability of employers to actively detect any behavioural irregularities or symptoms of stress or mental health problems due to the lack of face-to-face interaction.

Cases of discrimination against employees, or harassment, may also be difficult to detect, exposing employees to potential harm. Employers will need to establish clear processes and procedures for preventing and managing such incidents[11]. Another area of concern is employee data protection and privacy.

Cybersecurity concerns

Considering the buzz surrounding the metaverse, there is one critical component that is often overlooked: cybersecurity. It is easy to be caught up in the immersive and boundless virtual space that the metaverse creates, but one of the leading questions is 'what is keeping us and our data safe?'

Today's threat landscape is ever evolving and more dangerous than ever before. As attackers continue to use advanced methods that include artificial intelligence (AI) and machine learning to conduct attacks. At the same time, fledgling threat actors benefit from more accessible and affordable crime as a service product. When new technology emerges, there is always an exposed early threat, with an attacker only waiting to take advantage.



Whilst the metaverse remains in its infancy, taking cybersecurity seriously is critical. Customers are far more aware of the exposures faced using technology and make conscious decisions of whether to use a platform based on their knowledge. Should metaverse products or spaces suffer an attack the growth of the product, platform or general usage could be jeopardised. Therefore, whilst the interest of a brand/retailer entering the metaverse may be to protect itself, protecting the virtual identity of users should also be a priority. It is easy for us to take for granted how much information is transferred from customer to the company during traditional shopping methods; from an individual's height, weight, clothing preferences, credit card number, and bank account information.

Although some may not be stored in the physical world, they will be in the digital world. This is one of the key benefits to the metaverse as an active commercial environment; the value that can be obtained from an online location, accessing potential customers with their data could also make the metaverse a more desirable place to visit.

For the metaverse to thrive, a zero-trust model rooted in the concept must be adopted, from both the opinion of developers and those of the retailers that will feature; 'never trust, always verify'. A zero-trust model requires strict identity checks. It also uses ongoing authentication and verification to ensure threat actors are kept out or severely limited. With the colossal amounts of data set to be hosted in the metaverse, zero-trust is the most effective way to reduce or erase the theft of sensitive information.

For the metaverse to thrive, a zero-trust model rooted in the concept must be adopted, from both the opinion of developers and those of the retailers that will feature; 'never trust, always verify'.

Furthermore, AI plays a vital role in safeguarding the metaverse. For example, AI-driven cybersecurity tools can analyse user behaviour patterns across the network. However, this offers attackers an opportunity. When combining stolen personal information or collected open-source data, such as social media posts or online activity, cyber criminals can use AI to spread malware or collect valuable information.

Decentralisation technologies will likely be the go-to method when it comes to protecting user identities and intellectual property rights. Decentralisation is a crucial tenet of Web 3.0, with the idea being to restore user identities, data and property to their rightful owners, thereby putting power back in the hands of users.

While the metaverse will contain multiple software, users must invest in hardware like smart glasses and VR headsets to get the full user experience. This means robust cybersecurity measures for both the expanding digital and physical attack surfaces. It is only a matter of time before attackers can create lifelike digital deep fakes, and it will be incredibly difficult to identify the difference without sophisticated technology to analyse the source data. In essence, attackers will not be lacking in attack vectors; much like the presence itself for retailers.

While the future of the metaverse is still unknown, retailers should be aware of the privacy concerns it may bring. The global nature of the metaverse will challenge retailers to comply with a multitude of privacy regimes, while the novel structure of the metaverse will require them to collect and secure data in new ways. Retailers that are able to adapt to these privacy challenges may discover new opportunities in the metaverse.

Reputational damage

A brand's reputation is the driving force for customer acquisition and retention, as it differentiates major players in the market and offers them competitive leverage. Being exposed to millions of users, who are not only online but are also actively interacting with one another, could expose a business to significant reputational damage if any negative perceptions are shared against the brand.

The metaverse is similar to social media, whereby real-time and public customer-brand and customer-customer engagements could exacerbate a negative situation, making it difficult to contain. Such situations may arise due to various reasons, including unmonitored negative interactions between customers and employees in the metaverse, a mismatch between customer perceptions and brand offering, as well as false accusations and loss of credibility due to fake replicas etc.

Potential threats with regards to cyber security

People

Human Error and insider threat can compromise cyber secxurity.

Websites

Vulnerablilities to spoof websites, steal data and disrupt online activity.

Internet of things

Each connected device represents an attack surface and is an avenue for compromise.

Fine Websites & Digital Environments

Vulnerabilities to spoof websites, spoof stores & items, seal data and disrupt consumer online activity.

Contracts

Consider contractual obligations between you, your clients and any third parties such as metaverse platform providers.

Potential Metaverse related cybersecurity risks

- **Digital DNA Theft**
- **Theft of data**
- **Cyber attacks transfer between smart devices**
- **IP Infringement**
- **Strategies to thwart supply chain threats**
- **Camera based malware**
- **Jump of ransomware**
- **Weaponising operational technology environments**

The inability to meet customer expectations within the metaverse is a major concern. Customers have access to a wide range of products within the metaverse, which enables them to compare the varying options and choose those that best suit them. Product selection within that realm is not only based on the look of the product, but also the experience involved. Hence, if the overall experience does not complement the preconceived standard, customers will lose trust in the brand. Furthermore, brands offering phygital products, i.e. both physical and digital products, are particularly vulnerable as they can be scrutinised for the perceived differences between the two versions of the same product.

ESG concerns

Although by shifting into the metaverse retailers could reduce the costs of running a physical store, the associated environmental, social and governance implications could still be significant. Firstly, the technologies underpinning the infrastructure and transactions occurring in the metaverse consume significant amounts of energy, potentially resulting in greater carbon emissions than transacting physical items in the real world. Registering digital assets in the form of NFTs could have a massive environmental impact, whereby a single Ethereum transaction is shown to emit around 110kg of CO2, which is equivalent to 42,734 VISA transactions and watching over 18,000 hours of YouTube[12].

Furthermore, from a social aspect, there are various health and safety concerns with regards to users of the metaverse. As the metaverse becomes more appealing for users, and more hours are spent online, individuals could dissociate and disconnect from the real world, which could negatively impact their mental health. In addition, the technologies used to access some metaverse platforms, such as VR devices, could result in various health concerns, such as VR hangovers or post-VR sadness due to the level of stimulus and immersion that is involved in the experience in comparison to that in the real world – which could result in cyber addiction[13].

As the metaverse continues to develop and grow, criminals are expected to increasingly exploit the platforms for a plethora of illegal activities.

Moreover, due to the expenses, facilities, and technologies required to access the metaverse, the availability of such products is limited to a subsector of customers that have the necessary means. Hence, could be argued that there is an unfair selection for customer outreach, potentially discriminating against those that are incapable of meeting the requirements.

Crime

As the metaverse continues to develop and grow, criminals are expected to increasingly exploit the platforms for a plethora of illegal activities. A major concern is money laundering, as criminals use crypto transactions and other methods to launder illicit funds[14]. Moreover, detecting genuine versus fraudulent customers may be difficult due to the lack of direct interactions and the adopted mode for transacting. Criminals are finding ways to replicate or hijack user avatars within the metaverse[15], allowing them to carry out activities using other identities.

Moreover, sexual harassment and assault are atrocious acts, which unfortunately, are increasingly occurring across certain platforms due to the lack of monitoring and imposed restrictions. The list of possible crimes is growing, also including data theft, counterfeiting, ransomware and phishing attacks[16].

Managing the evolving risk landscape

Considering the changing operational landscapping a robust Enterprise Risk Management (ERM) approach, which helps retailers identify, assess, and mitigate both evolving and emerging risks is a matter of good governance. The full extent of how Web 3.0 and the metaverse will impact retail businesses is still unknown due to the infancy of the newly adopted technologies. However, businesses' can still enhance their preparedness and response strategies by undertaking systematic steps towards understanding the areas of impact and potential consequences.

Whether you have entered the metaverse, or seeking this opportunity in the future, understanding the infrastructure of the metaverse and the dynamics that exist within is necessary. Establishing your strategic objectives and aims for pursuing the metaverse as an operational environment and/or a marketing tool will verify the scope and context, as it sets out the extent of your exposure depending on the level of activities you will undertake and what you are looking to achieve.

As illustrated in the ISO 31000:2019 framework, risk management is a continuous process that evolves alongside the internal and external changes experienced by the business. Therefore, by adopting the metaverse as a new operational environment, updating the existing risk management approach to incorporate the potential implications is a must. That said, the appropriate risk identification and analysis techniques should be adopted. Subject matter experts and the relevant skillset should be involved throughout the process, to ensure all areas of exposure are adequately discussed, examined and addressed.

Diagram 1: ISO 31000:2019

Considering the pace of the metaverse's evolution, growth, as well as the increasing complexity of the technologies implemented, emerging risks are a major concern and should be accounted for in the ERM approach. Tools such as horizon scanning and scenario analysis should be utilised to ensure long-term view of the trajectory and materialisation of risks, as well as comprehensive assessment of the changing conditions that could trigger a new set of risks.

Systematically understanding and assessing the evolving risk landscape is crucial for effective resource allocation towards appropriate risk treatment strategies. As a retail business, understanding your internal risk appetite and tolerance will dictate whether to manage specific risks in-house or seek third-party protection, i.e. risk transfer. However, due to the limitations that exist within financial markets, and the terms and conditions imposed upon businesses for acquiring adequate protection, developing internal operational resiliency through ERM is a competitive advantage, especially during times of reduced market capacity.

Insurance solutions

Whilst there is yet to be a single insurance product for the metaverse, as discussed, the evolving risk landscape could impact existing insurance programmes and arrangements. This demonstrates the need reviewing the available solutions, to ensure that the business's needs are consistently met.

After discussing the implications of the metaverse with several global insurance carriers, it was evident that the lack of insight, knowledge and understanding created a sense of discomfort within the market. This is mainly due to the uncertainty associated with the metaverse as an operational environment, as well as the lack of relevant loss data to enable insurers to thoroughly understand the clients' risk portfolio.

Despite this, the use of the metaverse continues to expand rapidly, and the questions surrounding risk and insurance will grow as a consequence. Therefore, as we move forward, the insurance market seeks clarity to define and understand the risk, which might prompt new products and programme arrangements to emerge.

> Enhancing the staff's knowledge and understanding of the metaverse, as well as the deployed technologies and software systems, is crucial for ensuring smooth operation while protecting the staff against any potential exposures.

Considerations

- **Enhance and update your training programmes to accommodate for the evolving business model** upskilling staff is crucial for safely and comfortably operating within the metaverse. Enhancing the staff's knowledge and understanding of the metaverse, as well as the deployed technologies and software systems, is crucial for ensuring smooth operation while protecting the staff against any potential exposures.
- **Develop a strategy for platform selection** as the number of metaverse platforms increases, developing a strategy around which platform to select as your fully integrated omnichannel experience is crucial. Each platform attracts a different demographic depending on the features and experiences offered, hence it is important to ensure that the platform's outreach and capabilities are aligned to your strategic objectives.
- **Utilise the available data but ensure adequate data governance and regulatory compliance** whilst the metaverse could offer a vast selection of customer data, increasing your customer reach and providing you with customer insight, understanding the legal implications on a global scale is necessary to prevent potential regulatory scrutiny and loss of customer trust.
- **Protect your IP** whilst collaborating with customers to produce tailored products online is a massive opportunity for retailers, having comprehensive and clear contracts as to who owns any IP created in the metaverse, and the associated rights of each party, is detrimental. In addition, you must monitor any fake replicas in the metaverse that could jeopardise the authenticity of your products and your reputation.
- **Ensure that your ERM approach accounts for potential emerging risks your risk** management process should be consistent and frequent, involving all talent and stakeholders that have the necessary knowledge and experience to detect any evolving or emerging risks associated with operating in the metaverse. The approach should be continuously reviewed and improved in line with the rapidly changing operational environment and external circumstances. Ensuring adequate understanding and assessment of the new involved supply chain is particularly important.
- **Actively communicate any material changes to your business model with your risk advisors** to ensure that your insurance programme accounts for any developments in your risk landscape, consistent and transparent communication with your risk advisors is important early on in the process, to avoid potential disputes that could arise from associated claims. Moreover, risk professionals are more likely to have subject matter experts internally, or access to specialist expertise externally that could add value to a business, from both a risk management and insurance perspectives.
- **Keep up with the changing regulatory landscape.** Whilst there are no specific regulations governing the metaverse, the laws may change as it evolves and becomes more complex. Therefore, it is important to frequently seek the advice of legal advisors who have real-time knowledge and expertise that could safeguard a business against potential non-compliance and regulatory scrutiny. Moreover, due to the global outreach of metaverse platforms, businesses should be cautious of the varying global regulations that could apply to their operations and services within that realm. Therefore, keeping up with the changing global laws is also necessary.

References

1. https://www.businessleader.co.uk/mismatch-consumer-retailer-use-metaverse/
2. https://metaverse-timeline.com/
3. https://www.matthewball.vc/all/forwardtothemetaverseprimer
4. https://www.ey.com/en_gl/consumer-products-retail/meet-customers-in-the-metaverse-to-unlock-lasting-value
5. https://news.bitcoin.com/goldman-sachs-metaverse-8-trillion-opportunity/
6. https://www.businessleader.co.uk/mismatch-consumer-retailer-use-metaverse/
7. https://www.retail-week.com/retail-voice/three-stages-of-retail-opportunity-in-the-metaverse/7041806.article?authent=1#:~:text=Extending%20virtual%20worlds,by%2Dproduct%20of%20the%20experience.
8. https://www.businessleader.co.uk/mismatch-consumer-retailer-use-metaverse/
9. https://www.investopedia.com/non-fungible-tokens-nft-5115211
10. https://www.lexology.com/library/detail.aspx?g=f84b6476-beb2-4dec-a62f-9df00c1ae2b9
11. https://clarkslegal.com/insights/articles/the-metaverse-employment-law-implications/#:~:text=Employers%20will%20continue%20to%20be,working%20remotely%20via%20the%20Metaverse
12. https://medium.com/geekculture/how-green-is-the-metaverse-the-two-sides-of-the-environmental-impact-of-the-metaverse-6a35913fd329
13. https://www.forbes.com/sites/bernardmarr/2022/04/04/the-effects-of-the-metaverse-on-society/?sh=3bbec7ac765b
14. https://www.wolftheiss.com/insights/financial-crime-in-the-metaverse-is-real/#:~:text=The%20metaverse%20can%20be%20used,or%20metaverse%2Drelated%20crypto%20assets.
15. https://www.forbes.com/sites/bernardmarr/2022/11/18/policing-in-the-metaverse-whats-happening-now/?sh=1bad54752502
16. https://www.forbes.com/sites/bernardmarr/2022/11/18/policing-in-the-metaverse-whats-happening-now/?sh=1bad54752502

Get in touch

To learn more about any of the information above, or to find out how Lockton can help you mitigate these risks, please do not hesitate to get in touch with us.

Contact

Michael Kay
Head of Retail Practice
Lockton Companies LLP
E: michael.kay@lockton.com

Authors

Reem El Khatib
Risk and Research Manager
Lockton Companies LLP
E: reem.elkhatib@lockton.com

Jack Bassett
Assistant Vice President - Global Cyber and Technology, Lockton Companies LLP
E: jack.bassett@lockton.com

Co-authors

Cormac Bryce
Course Director MSc Insurance and Risk Management, Bayes Business School

Alvaro Ungaretti
MSc. Insurance and Risk Management, Bayes Business School

Independence changes everything

10953